BRIAN M. BOYNTON, Principal Deputy Assistant Attorney General
BURDEN H. WALKER, Acting Deputy Assistant Attorney General

AMANDA N. LISKAMM, Director
LISA K. HSIAO, Senior Deputy Director, Civil Litigation
ZACHARY A. DIETERT, Assistant Director

CAMERON A. BROWN, Trial Attorney
JAMES T. NELSON, Senior Trial Attorney
AMANDA K. KELLY, Trial Attorney
U.S. Department of Justice
Consumer Protection Branch
Civil Division
450 5th Street, N.W.
Washington, D.C. 20001
Telephone: (202) 514-9471
Cameron.A.Brown@usdoj.gov

ISMAIL J. RAMSEY (CABN 189820)
United States Attorney
MICHELLE LO (NYRN 4325163)
Chief, Civil Division
VIVIAN F. WANG (CABN 277577)
Assistant United States Attorney
United States Attorney's Office
Northern District of California
450 Golden Gate Ave.
San Francisco, CA 94102
Telephone: (415) 436-7431
vivian.wang@usdoj.gov

Attorneys for Plaintiff United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>VERKADA INC., a corporation,<br><br>Defendant. | Case No.: 3:24-cv-06153 CRB<br><br>**STIPULATED ORDER FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER EQUITABLE RELIEF** |

Plaintiff, the United States of America, acting upon notification and referral from the Federal Trade Commission ("Commission" or "FTC"), filed its Complaint for a permanent injunction, civil penalty judgment, and other equitable relief ("Complaint") in this matter, pursuant to Sections 5(m)(1)(A), 13(b), and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(m)(1)(A), 53(b), and 57b. Defendant has waived service of the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Order for Permanent Injunction, Civil Penalty Judgment, and Other Equitable Relief ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

**FINDINGS**

1. This Court has jurisdiction over this matter.

2. The Complaint charges that Defendant participated in deceptive and unfair acts or practices in violation of:

a. Section 5 of the FTC Act, 15 U.S.C. § 45 by:

i. failing to use appropriate information security practices to protect customers' and consumers' personal or sensitive information collected through the Defendant's security cameras or on the Command platform;

ii. misrepresenting that appropriate information security practices are maintained, and both HIPAA (the Health Insurance Portability and Accountability Act) compliance and/or certification and Privacy Shield compliance; and

iii. failing to disclose the association or current employment status with Defendant of employees who posted positive ratings and reviews about Defendant and its products online; and

b. Section 7(a) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C. § 7706(a) by:

i. failing to include a valid physical postal address in commercial electronic mail messages;

ii. failing to include unsubscribe links or other opt-out notice in commercial electronic mail messages; and

iii. failing to honor consumers' requests to opt out of receiving commercial electronic mail messages.

3. The monetary judgment entered against Defendant is a civil penalty for Defendant's violations of the CAN-SPAM Act alleged in the Complaint.

4. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.

5. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.

6. Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the validity of this Order.

**DEFINITIONS**

For the purpose of this Order, the following definitions apply:

A. **"Clear(ly) and Conspicuous(ly)"** means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made in only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that

it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.
6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

B. **"Commercial Electronic Mail Message"** means any Electronic Mail Message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).

C. **"Covered Incident"** means any incident that results in Defendant notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

D. **"Covered Product"** means (a) any security camera, building access control device, or other physical device designed, marketed, and offered by Defendant; and (b) the software used to access, operate, manage, or configure a device subject to part (a) of this definition, including, but not limited to, the firmware, web or mobile applications, and any related online services, that are advertised, developed, branded, or sold by Defendant, directly or indirectly.

E. **"Customer Information"** means the following information from or about an individual customer: (a) user account credentials, such as a login name and password and/or tokens; (b) email address; (c) a site floorplan; (d) name and title of customer contact; (e) Wi-Fi credentials; (f) a financial account number; (g) credit or debit card information; (h) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or a device or component serial number; (i) metadata about product usage (e.g., time, duration of video, IP address, location of camera); and (j) access control elements, including access levels, access groups, and badge numbers.

F. **"Defendant"** means Verkada Inc. and its successors and assigns.

G. **"Electronic Mail Address"** means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the "local part") and a reference to an Internet domain (commonly referred to as the "domain part"), whether or not displayed, to which an Electronic Mail Message can be sent or delivered.

H. **"Electronic Mail Message"** means a message sent to a unique Electronic Mail Address.

I. **"Personal Information"** means information from or about an individual consumer that Defendant collects through a Covered Product, including: (a) a first and last name; (b) a home or physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) date of birth; (f) usernames and passwords; (g) live camera footage; (h) video archives; (i) still images or photos; or (j) audio recordings.

## ORDER

### I. PROHIBITION AGAINST MISREPRESENTATIONS

**IT IS ORDERED** that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the marketing, advertising, promotion or offering, sale, or distribution of any product or service, are permanently restrained and enjoined from misrepresenting, expressly or by implication:

A. The extent to which Defendant maintains and protects the privacy, security, confidentiality, or integrity of any Personal Information or Customer Information;

B. The extent to which Defendant is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security or other compliance program sponsored by a government or any self-regulatory or standard-setting organization, or any entity that certifies compliance with HIPAA;

C. The extent to which Defendant is regulated by HIPAA, and the extent to which Defendant's privacy and information practices are in compliance with HIPAA requirements; and

D. The status of any person providing an endorsement or review of a product or service offered or sold by Defendant, or any business owned or controlled by Defendant, including a misrepresentation that the endorser or reviewer is an independent or ordinary user of the product or service or an ordinary customer of the business.

### II. MANDATED INFORMATION SECURITY PROGRAM

**IT IS FURTHER ORDERED** that Defendant and any business that Defendant controls directly, or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Personal Information or Customer Information, must, within sixty (60) days after entry of this Order, establish and implement, and thereafter maintain for twenty (20) years after entry of this Order, a comprehensive information security program ("Information Security Program") that protects

the security, confidentiality, and integrity of Personal Information and Customer Information. To satisfy this requirement, Defendant must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program;

B. Provide the written program and any material evaluations thereof or updates thereto to Defendant's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information and Customer Information that could result in the (1) unauthorized collection, maintenance, use, alteration, or disclosure of, or provision of access to, Personal Information or Customer Information; or the (2) misuse, loss, theft, destruction, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Defendant identifies to the security, confidentiality, or integrity of Personal Information and Customer Information identified in response to Provision II.D. Each safeguard shall be based on the volume and sensitivity of the Personal Information or Customer Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, alteration, or disclosure of the Personal Information or Customer Information; or the (2) misuse, loss, theft, destruction, or other compromise of such information. Such safeguards must also include:

1. Training of all of Defendant's employees, at least once every twelve (12) months, on how to safeguard Personal Information and Customer Information;

2. Implementing technical measures to log and monitor Defendant's networks and assets for anomalous activity and active threats. Such measures shall require Defendant to determine baseline system activity and identify and respond to anomalous events and unauthorized attempts to access or exfiltrate Personal Information or Customer Information;
3. Implementing data access controls for all assets (including databases) storing Personal Information or Customer Information and technical measures, policies, and procedures to minimize or prevent online attacks resulting from the misuse of valid credentials, including: (a) restricting inbound and outbound connections; (b) requiring and enforcing strong passwords or other credentials; (c) preventing the reuse of known compromised credentials to access Personal Information or Customer Information; (d) implementing routine password resets for known compromised credentials; and (e) limiting employee, contractor, or authorized third party access to what is needed to perform that employee, contractor, or authorized third party's job function and establish regular documented review of such access privileges;
4. Requiring multi-factor authentication methods for all employees, contractors, and affiliates in order to access any assets (including databases) storing Personal Information or Customer Information. Such multi-factor authentication methods for all employees, contractors, and affiliates should not include telephone calls or SMS-based authentication methods and must be resistant to phishing attacks. Defendant may use equivalent, widely-adopted industry authentication options that are not multi-factor, if the person responsible for the Information Security Program under sub-Provision II.C: (1) approves in writing the use of such equivalent authentication options; and (2) documents a written explanation of how the authentication options are widely adopted and at least equivalent to the security provided by multi-factor authentication;
5. Developing and implementing configuration standards to harden system components against known threats and vulnerabilities. New system components shall not be granted access to

Defendant's network, resources, Personal Information, or Customer Information until they meet Defendant's configuration standards;

6. Encryption of, at a minimum, all Personal Information and Customer Information on Defendant's computer networks, including but not limited to cloud storage;
7. Policies and procedures to ensure that all information technology ("IT") assets on Defendant's network with access to Personal Information or Customer Information are securely installed and inventoried at least once every twelve (12) months;
8. Implementing vulnerability and patch management measures, policies, and procedures that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed and that include timelines for addressing vulnerabilities that account for the severity and exploitability of the risk implicated.
9. Identify and document a comprehensive IT asset inventory that includes hardware, software, and location of the assets;
10. Designing and implementing protections such as network intrusion protection, host intrusion protection, and file integrity monitoring, across Defendant's network and IT assets;
11. Designing, implementing, and maintaining measures to limit unauthorized access in any network or system that stores, collects, maintains, or processes Personal Information or Customer Information, such as segmentation of networks and databases and properly configured firewalls; and
12. Technical measures, procedures, and policy provisions to address the maintenance of any type of information related to customers that was not being collected or maintained by Defendant as of the entry date of this Order, including a determination of whether the safeguards that control for the internal and external risks to the security, confidentiality, or integrity of Customer Information should be applied to this new type of information.

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal

and external risks to the security, confidentiality, or integrity of Personal Information and Customer Information, and modify the Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability testing of Defendant's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after a Covered Incident, and penetration testing of Defendant's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Personal Information and Customer Information they access through or receive from Defendant, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Personal Information and Customer Information; and

I. Evaluate and adjust the Information Security Program in light of any changes to Defendant's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision II.D of this Order, or any other circumstances that Defendant knows or has reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, Defendant must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

## III. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

**IT IS FURTHER ORDERED** that, in connection with compliance with Provision II of this Order titled Mandated Information Security Program, Defendant must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the

profession; (2) conducts an independent review of the Information Security Program; (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.

B. For each Assessment, Defendant must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the entry date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after entry of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period:

1. Determine whether Defendant has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program;
2. Assess the effectiveness of Defendant's implementation and maintenance of sub-Provisions II.A-I;
3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;
4. Address the status of gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and
5. Identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate

for assessing an enterprise of Defendant's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Defendant's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Defendant's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Defendant revises, updates, or adds one or more safeguards required under Provision II of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Defendant must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "United States v. Verkada Inc., FTC File No. 2123068." All subsequent biennial Assessments must be retained by Defendant until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

## IV. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR

**IT IS FURTHER ORDERED** that Defendant, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Information Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Defendant's network(s), systems, and IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s), systems, and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Defendant has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

## V. ANNUAL CERTIFICATION

**IT IS FURTHER ORDERED** that Defendant must:

A. One (1) year after the entry date of this Order, and each year thereafter for twenty (20) years after entry of this Order, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Verkada Inc. responsible for Defendant's Information Security Program that: (1) Defendant has established, implemented, and maintained the requirements of this Order; (2) Defendant is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of

Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "United States v. Verkada Inc., FTC File No. 2123068."

## VI. COVERED INCIDENT REPORTS

**IT IS FURTHER ORDERED** that, for twenty (20) years after entry of this Order, within ten (10) days of any notification to a United States federal, state, or local entity of a Covered Incident, Defendant must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that was affected by the Covered Incident;

D. The number of consumers whose information was affected by the Covered Incident;

E. The acts that Defendant has taken to date to remediate the Covered Incident and protect Personal Information and Customer Information from further exposure or access, and protect affected consumers from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of any materially different notice sent by Defendant to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "United States v. Verkada Inc., FTC File No. 2123068."

## VII. PROHIBITIONS CONCERNING COMMERCIAL EMAIL

**IT IS FURTHER ORDERED** that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, marketing,

promotion, offering for sale, or sale of any product, service, or program, are permanently restrained and enjoined from violating Section 5 of the CAN-SPAM Act, 15 U.S.C. § 7704, a copy of which is attached hereto as Exhibit A, by, including but not limited to:

A. Initiating, procuring, or transmitting, or assisting others in initiating, procuring, or transmitting, a Commercial Electronic Mail Message that does not: (1) provide a physical postal address of the sender, or (2) provide a Clear and Conspicuous notice of opportunity to decline to receive further Commercial Electronic Mail Messages from the sender; and

B. Failing to honor a recipient's request not to receive further Commercial Electronic Mail Messages from Defendant at the recipient's Electronic Mail Address more than 10 business days after the recipient's request.

## VIII. MONETARY JUDGMENT FOR CIVIL PENALTY

**IT IS FURTHER ORDERED** that:

A. Judgment in the amount of two million nine hundred fifty thousand dollars ($2,950,000) is entered in favor of Plaintiff against Defendant as a civil penalty.

B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the United States, $2,950,000 which as Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment to Plaintiff. Such payment must be made within seven (7) days of entry of this Order by electronic fund transfer in accordance with instructions to be provided by a representative of Plaintiff.

## IX. ADDITIONAL MONETARY PROVISIONS

**IT IS FURTHER ORDERED** that:

A. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission or Plaintiff, including in a proceeding to enforce its rights to any payment or monetary judgment pursuant to this Order.

C. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security Number or

Employer Identification Numbers), which Defendant previously submitted to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

## X. ORDER ACKNOWLEDGMENTS

**IT IS FURTHER ORDERED** that Defendant obtain acknowledgments of receipt of this Order:

A. Defendant, within seven (7) days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For ten (10) years after entry of this Order, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who have managerial responsibility for conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Defendant delivered a copy of this Order, Defendant must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

## XI. COMPLIANCE REPORTING

**IT IS FURTHER ORDERED** that Defendant make timely submissions to the Commission:

A. One year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury, which does the following: (1) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission and Plaintiff may use to communicate with Defendant; (2) identify all of Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and

services offered, the means of advertising, marketing, and sales; (4) describe in detail whether and how Defendant is in compliance with each Provision of this Order; and (5) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

B. For twenty (20) years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in: (1) any designated point of contact; or (2) the structure of Defendant or any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Defendant within fourteen (14) days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "United States v. Verkada Inc., FTC File No. 2123068."

## XII. RECORDKEEPING

**IT IS FURTHER ORDERED** that Defendant must create certain records for twenty (20) years after entry of the Order, and retain each such record for five (5) years. Specifically, Defendant must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each individual working for Defendant, whether as an employee or otherwise, that individual's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Records of all consumer complaints and refund requests concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;

D. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission;

E. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

F. A copy of each unique Commercial Electronic Mail Message template making a representation subject to this Order;

G. Records sufficient to show, by campaign, the number of Commercial Electronic Mail Messages sent, and the notice provided to Commercial Electronic Mail Message recipients of the opportunity to unsubscribe from the receipt of further Commercial Electronic Mail Messages;

H. Records sufficient to show that each Commercial Electronic Mail Message recipient's unsubscribe request, submitted via the manner specified in the Commercial Electronic Mail Message, has been honored no more than ten (10) business days after receipt of such request, or if not, for each such request, the date of the request, date of each subsequent Commercial Electronic Mail Message, the reason the request was not honored, and a copy of the Commercial Electronic Mail Message; and

I. Records sufficient to show the number of Commercial Electronic Mail Messages, by campaign, that (1) included the sender's valid physical postal address, and (2) did not include the sender's valid physical postal address.

## XIII. COMPLIANCE MONITORING

**IT IS FURTHER ORDERED** that, for the purpose of monitoring Defendant's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission or Plaintiff, Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission and Plaintiff are also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission and Plaintiff are authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission and Plaintiff to interview any employee or other person affiliated with Defendant who has agreed to such an interview. The person interviewed may have counsel present.

C. The Commission and Plaintiff may use all other lawful means, including posing, through their representatives as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

## XIV. RETENTION OF JURISDICTION

**IT IS FURTHER ORDERED** that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

**SO ORDERED this** 4th **day of** September **20**24

UNITED STATES DISTRICT JUDGE

**SO STIPULATED AND AGREED:**

**FOR PLAINTIFF:**

**THE UNITED STATES OF AMERICA**

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General, Civil Division

BURDEN H. WALKER
Acting Deputy Assistant Attorney General, Civil Division

AMANDA N. LISKAMM
Director, Consumer Protection Branch

LISA K. HSIAO
Senior Deputy Director, Civil Litigation

ZACHARY A. DIETERT
Assistant Director

*/s/ Cameron A. Brown* Date: August 30, 2024
CAMERON A. BROWN, Trial Attorney
JAMES T. NELSON, Senior Trial Attorney
AMANDA K. KELLY, Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W.
Washington, D.C. 20001
Telephone: (202) 514-9471
Email: Cameron.A.Brown@usdoj.gov

ISMAIL J. RAMSEY
United States Attorney
Northern District of California

*/s/ Vivian F. Wang* Date: August 30, 2024
VIVIAN F. WANG
Assistant U.S. Attorney
United States Attorney's Office
for the Northern District of California
Tel: (415) 436-7431
Email: vivian.wang@usdoj.gov

Of Counsel:

BENJAMIN WISEMAN
Associate Director
Division of Privacy and Identity Protection

TIFFANY GEORGE
Assistant Director
Division of Privacy and Identity Protection

JACQUELINE K. FORD
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-2844 (voice)
(202) 326-3062 (fax)

KAMAY LAFALAISE
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-3780 (voice)
(202) 326-3062 (fax)

**FOR DEFENDANT, VERKADA INC.:**

Date: August 29, 2024

JANIS CLAIRE KESTENBAUM
Perkins Coie LLP
700 13th Street, N.W., Suite 800
Washington, D.C. 20005
(202) 654-6200
JKestenbaum@perkinscoie.com

Date: August 29, 2024

REBECCA S. ENGRAV
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
(206) 359-6168
REngrav@perkinscoie.com

EDITH RAMIREZ
CHUCK LOUGHLIN
Hogan Lovells US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5509 (Ramirez)
(202) 637-5661 (Loughlin)
edith.ramirez@hoganlovells.com
chuck.loughlin@hoganlovells.com

**VERKADA INC.:**

Date: August 29, 2024

BILL BERRY
GENERAL COUNSEL OF VERKADA INC.

# Exhibit B

**REASONS FOR SETTLEMENT**

This statement accompanies the Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Equitable Relief ("Order") executed by defendant Verkada Inc. ("Defendant") in settlement of an action seeking injunctive relief, civil penalties, and other relief for Defendant's violations of Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C. §§ 7701-7713. The Order imposes injunctive relief and requires Defendants pay $2,950,000 as a civil penalty.

Pursuant to Section 5(m)(3) of the FTC Act, 15 U.S.C. § 45(m)(3), the Commission hereby sets forth its reasons for settlement by entry of the Order:

Based on the allegations contained in the Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Equitable Relief, and the factors set forth in Section 5(m)(1)(C) of the FTC Act, 15 U.S.C. § 45(m)(1)(C), the Commission believes that entry of the Order is appropriate and in the public interest.

First, the $2,950,000 civil penalty and the injunctive provisions in the Order constitute an effective means to ensure Defendant's future compliance with the law and deter others from engaging in similar violations.

Second, the Order is consistent with past orders entered in cases involving similar violations of the FTC Act and the CAN-SPAM Act.

Finally, with the entry of the Order, the time and expense of litigation against Defendant will be avoided.

For the foregoing reasons, the Commission believes that settlement by entry of the attached Order is justified and well within the public interest.